

7le



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,532	07/14/2001	Antony John Rogers	063170.6291	3485
5073	7590	07/17/2006	EXAMINER	
BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980			SCHUBERT, KEVIN R	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 07/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/905,532

Applicant(s)

ROGERS ET AL.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4,5,8-17 and 20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4,5,8-17 and 20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

Art Unit: 2137

b) creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values (Col 9, lines 13-32);

5 c) emulating execution of at least a portion of computer executable code in a subject file (Col 3, lines 42-45);

d) monitoring operating system calls by the emulated computer executable code (Col 6, line 68; Col 7, lines 1-15);

e) identifying a type of operating system call that the emulated computer executable code attempted to access (Col 9, lines 13-25; Col 9, lines 44-54);

10 f) deciding, based on the type of operating system call identified, whether the emulated computer executable code comprises viral code (Col 9, lines 13-25; Col 9, lines 44-54);

As per claims 4 and 16, the applicant discloses the method of claim 1, which is met by Chambers (see above), with the following limitations which are also met by Chambers:

15 emulating functionality of the identified operating system call while monitoring the operating system call to determine whether the computer executable code is viral (Col 9, lines 13-25; Col 9, lines 44-54);

20 As per claims 5 and 17, the applicant discloses the method of claim 1, which is met by Chambers (see above), with the following limitations which are also met by Chambers:

a) monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping in the execution of the emulated computer executable code (Col 3, lines 51-53; Col 3, line 64 to Col 4, line 14);

25 b) determining based on a detection of looping whether the emulated computer executable code is viral (Col 3, lines 51-53; Col 3, line 64 to Col 4, line 14).

Art Unit: 2137

As per claims 13 and 15, the applicant discloses the method of claims 12 and 14 respectively, which are met by Chambers (see above), with the following limitations which are also met by Chambers:

a) a fourth segment comprising auxiliary code, wherein the auxiliary code determines an operating system call that the emulated computer executable code attempted to access (Col 9, lines 13-25; Col 9, lines 44-54);

b) a fifth segment comprising analyzer code, wherein the analyzer code monitors the operating system call to determine whether the computer executable code is viral, while emulation continues (Col 9, lines 13-25; Col 9, lines 44-54);

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 8, 9, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chambers in further view of Golan, U.S. Patent No. 5,974,549.

As per claim 8, the applicant describes the method of claim 1, which is anticipated by Chambers (see above), with the following limitation which is anticipated by Golan:

Further comprising monitoring access by the emulated computer executable code to dynamically linked functions (Col 6, lines 6-12; Col 5, lines 60-63);

Chambers describes all the limitations of claim 1, the independent claim. However, Chambers fails to disclose anything concerning dynamically linked functions. Golan describes a security monitor method whereby access to dynamically linked functions is regulated because, as Golan discloses, "in an operating system that supports virtual memory and hardware abstraction, a software component can only

Art Unit: 2137

breach security by calling a system call" (Col 5, lines 38-41). It would have been obvious to one of ordinary skill in that art at the time the invention was filed to have combined the teachings of Chambers with those of Golan and monitor access to dynamically linked functions because requesting access to dynamically linked functions could be an attempt to breach security.

5

As per claim 9, the applicant discloses the method of claim 8, which is met by Chambers in further view of Golan (see above), with the following limitation which is met by Golan:

Wherein the artificial memory region spans a jump table containing pointers to the dynamically linked functions (Col 7, lines 31-35);

10 Chambers in further view of Golan describes all the limitations of claim 8. Golan describes the additional limitation of a jump table containing pointers to the dynamically linked functions. The jump table is often incorporated with dynamically linked functions to store the actual addresses of the dynamically linked functions. It would have been obvious to one of ordinary skill in the art at the time in the invention was filed to have included a jump table with the method so that there could be a way of
15 storing the actual addresses of the dynamically linked functions.

As per claim 20, the applicant discloses the method of claim 14, which is met by Chambers (see above), with the following limitation which is met by Golan:

20 Wherein the artificial memory region created by the memory manager component spans a jump table containing pointers to dynamically linked functions, and the monitor component monitors access by the emulated computer executable code to the dynamically linked functions;

The claim is met by the combination of claims 8 and 9. Explanations for claim 8 and 9 rejections are listed above.

25

Response to Arguments

Art Unit: 2137

Applicant's arguments, see Remarks filed 5/22/06, with respect to the 102(b) rejection of claim 1 under Chambers have been fully considered but they are not persuasive. Applicant presents the following argument:

1) Chambers does not identify a type of operating system call

5 2) Chambers does not decide whether code is viral based on the type of operating system call

Examiner respectfully disagrees. Prior to the instant amendment, Examiner rejected claim 1 under Chambers as teaching identifying an operating system call and deciding whether code is viral based on the operating system call. In the instant Remarks, Applicant does not appear to contest the
10 foregoing. Rather, Applicant appears to contest that no *type of* operating system call is identified. Examiner fails to see how Chambers identifies operating system calls but not types of operating system calls or how Chambers makes a viral determination based on operating system calls but not types of operating system calls, especially in light of the following.

Chambers discloses a method of detecting computer viruses. The detection method utilizes a
15 monitor program to analyze target code. In particular, the monitor program may determine whether target code replaces an interrupt handler with a routine of its own (Col 9, lines 23-25). The interrupt handlers represent operating system calls. If replacement of an interrupt handler occurs, the method "sacrifices" a guinea pig file to a potential viral interrupt handler (Col 9, lines 62-64). The potential viral interrupt handler executes, thereby executing operating system calls, and a determination is made as to whether
20 the potential interrupt handler is viral based on the type of calls executed (e.g. if the calls modify the content of the guinea pig file) (Col 9, line 62 to Col 10, line 19, especially Col 10, lines 17-19). Thus, Chambers teaches 1) identifying a type of operating system call and 2) deciding whether code is viral based on the type of operating system call.

The Examiner further notes that the above is merely one example in Chambers which meets the
25 claim language. In response to Applicant's argument that Chambers teaches identifying calls to change operating system entry points, not identifying types of operating system calls, Examiner respectfully disagrees. Examiner disagrees that identifying a call to change an os entry point is not identifying a type

Art Unit: 2137

of os call, but, even assuming arguendo that all of Applicant's Remarks are correct, Examiner notes that the claim language is still met as described above.

For at least these reasons, Examiner disagrees and maintains the previous rejection.

5 Applicant's arguments with respect to the 102(b) rejection of claim 5 under Chambers have been fully considered, but they are not persuasive. Applicant's argument has been carefully considered, but Examiner notes that this argument has already been addressed. See action mailed 10/31/05, page 7, lines 9-28.

10 **Conclusion**

This action is made non-final. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

15 If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

20 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

25 KS


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER